

La Rom Craking

Par Claude S. et André C.

C'est le petit nom familial donné à cette Rom par Claude, parce qu'au boot elle affiche :

CRACKING SERVICE & C

© 1985 MANDARINE

Ce petit bijou original est l'œuvre de François S., le fils de Claude. Comme l'indique le ©, elle date de 1985 et François n'était encore qu'un petit garçon, certes un peu doué...

En fait, l'appellation "Rom craking" est un peu inappropriée. Il faudrait plutôt l'appeler "Rom de communication RS232 entre deux Atmos", mais bon, ça ne retire rien à la chose.

QUE FAIT LA ROM CRACKING?

Elle permet d'envoyer ou de recevoir des fichiers Oric sur une carte RS232 en utilisant la syntaxe usuelle de CLOAD/CSAVE. La carte doit être branchée sur le connecteur d'extension et non sur la prise K7. La vitesse de transmission est de 115200 bauds (horloge externe), mais il est possible de travailler à 9600 bauds, en utilisant le paramètre ",S". Il est donc possible de communiquer entre 2 Oric si l'on dispose de 2 cartes RS232. Les cartes utilisées doivent décoder les adresses 0320 à 0323.

Les modifications apportées aux commandes CSAVE"" et CLOAD"" sont limitées. Normalement ces commandes analysent la syntaxe, configurent le VIA, affichent "Saving..." ou "Searching...", sauvent ou cherchent l'entête (et



affichent "Loading" quand elle est trouvée), sauvent ou chargent le fichier et enfin reconfigurent le VIA. L'enregistrement ou la détection de la bande amorce (pour synchroniser l'interface K7) est supprimée. A la place, CLOAD envoie un #FF pour indiquer qu'il est prêt à recevoir et CSAVE attend un #FF avant d'envoyer le fichier précédé de son entête usuelle. Enfin, au lieu de passer pas mal de temps à élaborer ou à décoder les créneaux qui constituent le signal K7, le nouveau code se contente d'initialiser la carte et de placer ou de lire les octets dans le registre data du 6551. Le nouveau code est beaucoup plus concis que l'ancien et donc plus rapide.

MODIFICATIONS APPORTÉE A UNE ROM NORMALE:

Dans ce qui suit, les adresses indiquées sont situées en Ram (le fichier qui se trouve normalement en Rom de C000 à FFFF a été chargé en Ram de 2000 à 5FFF).

1) Commande CLOAD, sous-programme "Charger un programme" qui va normalement de E4E0 à E50A. De E4E0 à E4EB, il place en 33/34 l'adresse de début du bloc à charger. Puis il initialise le pointeur Y=#00 et à partir de E4EC, il charge les octets un à un, jusqu'à la fin. Un détour sera ajouté en E4E8 afin qu'il envoie d'abord le drapeau "Prêt à recevoir". Le retour au cours normal des choses se fera en E4EC.

44E8	84 34	STY 34	devient	4C 4A E7	JMP E74A	adresse de la routine Envoyer
44EB	A0 00	LDY #00		EA	NOP	le drapeau "Prêt à recevoir"

2) Commande CSAVE, sous-programme "Sauver l'entête" qui va normalement de E607 à E62D est légèrement modifié. En E607, le JSR E75A ("Sauver la bande amorce") est remplacé par un JSR E735 ("Initialiser la carte RS232").

4607	20 5A E7	JSR E75A	devient	20 35 E7	JSR E735	adresse de la nouvelle routine
------	----------	----------	---------	----------	----------	--------------------------------

3) Commande CSAVE, sous-programme "Sauver un programme" qui va normalement de E62E à E644. De E62E à E637, il place en 33/34 l'adresse de début du bloc à sauver. Puis il initialise le pointeur Y=#00 et à partir de E63A, il sauve les octets un à un, jusqu'à la fin. Un détour sera ajouté en E636 afin d'attendre l'arrivée du drapeau "Prêt à recevoir". Le retour au cours normal des choses se fera en E63A.

4636	84 34	STY 34	devient	4C 6B E6	JMP E66B	adresse de la routine Attendre
4639	A0 00	LDY #00		EA	NOP	le drapeau "Prêt à recevoir"

4) Commande CSAVE, sous-programme "Ecrire un octet" qui va normalement de E65E à E68A. Il a été complètement re-écrit et va maintenant de E65E à E66A:

465E	85	devient	48	PHA	sauve l'octet
465F	2F 8A 48		AD 21 03	LDA 0321	registre d'état
4662	98 48		29 10	AND #10	teste si prêt à émettre
4664	20 C0		F0 F9	BEQ 465F	sinon, reboucle
4666	E6		68	PLA	si oui, récupère l'octet
4667	18 A0 09		8D 20 03	STA 0320	le met dans le registre d'émission
466A	A9		60	RTS	et retourne

La routine "Attendre le drapeau Prêt à recevoir" a été insérée dans la place restante:

466B	00 F0	devient	84 34	STY 34	restauration du code écrasé en 4636
466D	06 46 2F		20 C9 E6	JSR E6C9	"Prendre un octet"
4670	08 69		C9 FF	CMP #FF	est-ce un #FF?
4672	00 28		D0 F9	BNE 466D	si non, reboucle en E66D
4674	20 8B		A2 03	LDX #03	si oui,
4676	E6 88		A0 FF	LDY #FF	lance
4678	D0		88	DEY	une boucle
4679	F4 49		D0 FD	BNE 4678	de temporisation
467B	01		CA	DEX	d'environ
467C	4A A0		D0 F8	BNE 4676	4 secondes
467E	04 20		A0 00	LDY #00	restauration du code écrasé en 4638
4680	8B E6 38		4C 3A E6	JMP E63A	reprend cours normal du sous-prog "Sauver un programme" en E63A. La fin inchangée de l'ancien code, de E683 à E68A, restera inutilisée.

5) Commande CLOAD, sous-programme "Prendre un octet" va normalement de E6C9 à E6FB. La carte faisant le travail effectué anciennement par le soft, ce sous-programme est simplifié comme suit:

46C9	98 48 8A	devient	AD 21 03	LDA 0321	lit registre d'état
46CC	48 20		29 08	AND #08	et le teste
46CE	1C E7		F0 F9	BEQ 46C9	reboucle si rien reçu
46D0	20 1C E7		AD 20 03	LDA 0320	lit l'octet reçu dans le registre de réception
46D3	B0		60	RTS	et retourne

La fin inchangée de l'ancien code, de E6D4 à E6FB, restera inutilisée.

6) Commande CLOAD, sous-prog "Trouver la bande amorce" situé de E735 à E759. Puisqu'on n'a plus besoin de bande amorce, il est remplacé par un nouveau sous-prog: "Initialiser la carte RS232". C'est ici qu'il faudra intervenir pour changer éventuellement les paramètres de transmission:

4735	20 FC	devient	A9 65	LDA #65	parité paire, pas de RTS, IRQ valide
4737	E6 66 2F		8D 22 03	STA 0322	registre de commande
473A	A9 16 C5		AD 4D 02	LDA 024D	flag à 0 si mode "FAST"
473D	2F D0		D0 05	BNE 4744	si le paramètre ",S" est en cours
473F	F5 AD		A9 10	LDA #10	si nul, horloge externe (voir *)
4741	4D 02 F0		4C 46 E7	JMP E746	et reprend le cours normal en E746
4744	08 20		A9 1E	LDA #1E	si ",S": 9600 bauds, 8 bits, 1 stop
4746	1C E7 20		8D 23 03	STA 0323	registre de contrôle
4749	1C		60	RTS	et retourne

NB* La vitesse utilisée est 1/16e de la fréquence du quartz soit 1843200 / 16 = 115200 bauds

La routine "Envoyer le drapeau Prêt à recevoir" a été insérée dans la place restante en E74A:

474A	E7 B0	devient	84 34	STY 34	restauration du code écrasé en 44E8
474C	FB A2		A0 00	LDY #00	restauration du code écrasé en 44EA
474E	03 20		A9 FF	LDA #FF	drapeau "Prêt à recevoir"
4750	C9 E6 C9		20 5E E6	JSR E65E	"Ecrire un octet"
4753	16 D0 DF		4C EC E4	JMP E4EC	reprend le cours normal du sous-
4756	CA D0		EA EA	NOP NOP	programme "Charger un programme"
4758	F6 60		EA EA	NOP NOP	

7) Commande CLOAD/CSAVE, sous-progr "Comparer le nom demandé et le nom trouvé". situé de E790 à E7AE. Il a été légèrement modifié afin de supprimer une bogue: le nom demandé était systématiquement recopié dans le nom trouvé, ce qui n'avait pas de sens, particulièrement lorsque les noms étaient différents! Voici en gras les octets à modifier:

```
Searching ... CAPS
ORIC CRAKING SERVICE & C
© 1985 MANDARINE

37631 BYTES FREE

Ready
CLOAD""
█
```

```
Saving ... ESSAI B CAPS
ORIC CRAKING SERVICE & C
© 1985 MANDARINE

37631 BYTES FREE

Ready
CSAVE"ESSAI",AUTO
█
```

4797	F0 15	devient	F0 09	BEQ 47A2	1er octet du nom demandé était nul
4799	B9 7F 02		B9 7F 02	LDA 027F,Y	lit un octet du nom demandé
479C	D9 93 02		D9 93 02	CMP 0293,Y	compare avec homologue du nom trouvé
479F	F0 01		F0 02	BEQ 47A3	by-passe les 2 instr. suiv. si identiques
47A1	E8		E8	INX	s'ils sont différents: X <> 0
47A2	99		60	RTS	retourne immédiatement
47A3	93		C8	INY	vise l'octet suivant
47A4	02 C8		C0 11	CPY #11	jusqu'a un maximum de 16 octets
47A6	C0 11		F0 FA	BEQ 47A2	retourne si fini
47A8	B0 04 48		4C 99 E7	JMP E799	pas fini, continue à comparer
47AB	68 D0 EB		EA EA EA	NOP NOP NOP	
47AE	60		60	RTS	

NB Les nom de fichiers se terminent par #00. Si la chaîne est vide (pas de nom), il y a seulement ce #00.

8) COPYRIGHT

Le message de copyright a été modifié:

En ED9B les octets 45 58 54 45 4E 44 45 4420 42 41 53 49 43 20 56 31 2E 31 0D 0A soit EXTENDED BASIC V1.1 deviennent (en 4D9B) 43 52 41 4B 49 4E 47 20 53 45 52 56 49 43 45 20 26 20 43 0D 0A soit CRAKING SERVICE & C
Et en EDB0 les octets 60 20 31 39 38 33 20 54 41 4E 47 45 52 49 4E 45 0D 0A 00 soit © 1983 TANGERINE deviennent (en 4DB0) 60 20 31 39 38 35 20 4D 41 4E 4441 52 49 4E 45 0D 0A 00 soit © 1985 MANDARINE

9) PAPER/INK

5914	A9 07	LDA #07	encre noire (#00) devient blanche (#07)
5916	8D 6C 02	STA 026C	
5919	A9 14	LDA #14	papier blanc (#17) devient bleu (#14)
591B	8D 6B 02	STA 026B	

